IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant:	Nancy Cam-Winget et al.		
Assignee:	Atheros Communications, Inc.		
Title:	Key Refresh At The MAC Layer		
Serial No.:	10/086,029	File Date:	February 27, 2002
Examiner:	Syed Zia	Art Unit:	2131
Docket No.:	ATH-0073		

February 13, 2008

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

This Appeal Brief is in support of the Notice of Appeal dated February 13, 2008.

/

/

/

/

/

/

/

/

/

/

/

INDEX

I. REAL PARTY IN INTEREST

The real party in interest is the assignee, Atheros Communications, Inc., pursuant to the Assignment recorded in the U.S. Patent and Trademark Office on February 27, 2002 on Reel 012672, Frame 0017.

II. RELATED APPEALS AND INTERFERENCES

Based on information and belief, there are no other appeals or interferences that could directly affect or be directly affected by or have a bearing on the decision by the Board of Patent Appeals in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-41 are pending. Claims 1-9, 14, 16-17, 20-30, 33, 35-38, and 41 are rejected. Claims 10-13, 15, 18-19, 31-32, 34, and 39-40 are objected to as being dependent on rejected base claims, but would be allowable if rewritten and merged with their respective base claims and any intervening claims.

In the present paper, rejected Claims 1-41 are appealed.

Pending Claims 1-41 are listed in the Claims Appendix.

IV. STATUS OF AMENDMENTS

All claim amendments have been entered.

V. SUMMARY OF CLAIMED SUBJECT MATTER

A concise explanation of the subject matter defined in each of the independent claims involved in the appeal (i.e. **Claims 1, 26, and 37**) is provided below. This concise explanation provides exemplary, non-limiting references to the specification by paragraph, page, and line numbers, and to the drawings by reference numbers.

Claim 1. A method [**Figure 3: 300; Specification: paragraphs 0017-0021, page 6, line 1 to page 8, line 2**] for encrypted communications between a first transceiver and a second transceiver [**Figure 2: 211, 221, 231; Specification: paragraphs 0015-0016, page 5, lines 4-31**], the method comprising.

sending from a first transceiver to a second transceiver a request to initiate derivation of a new encryption key [**Figure 4: 400; Specification: paragraph 0023, page 8, line 20 to page 9, line 4**], the request to initiate a new encryption key derivation being controlled by a MAC sub-layer and including an exchange threshold indicative of when the new encryption key is to be used to encrypt communication packets [**Figure 1: 102A; Figure 4: 400; Specification: paragraph 0022, page 8, lines 3-19; paragraph 0023, page 8, line 20 to page 9, line 4**].

Claim 26. A first transceiver that is to conduct encrypted communications with a second transceiver [**Figure 2: 211, 221, 231; Specification: paragraphs 0015-0016, page 5, lines 4-31**], the first transceiver comprising:

a physical control layer that sends to the second transceiver a request to initiate derivation of a new encryption key, the request to initiate a new encryption key derivation being controlled by a MAC sub-layer and including an exchange

threshold indicative of when the new encryption key is to be used to encrypt communication packets [**Figure 1: 102A; Figure 4: 400; Specification: paragraph 0022, page 8, lines 3-19; paragraph 0023, page 8, line 20 to page 9, line 4**].

Claim 37. A first transceiver that is to conduct encrypted communications with a second transceiver [**Figure 2: 211, 221, 231; Specification: paragraphs 0015-0016, page 5, lines 4-31**], the first transceiver comprising:

a physical control layer that receives from the second transceiver a request to initiate derivation of a new encryption key, the request to initiate a new encryption key derivation being controlled by a MAC sub-layer and including an exchange threshold indicative of when the new encryption key is to be used to encrypt communication packets, and a first nonce needed to derive the new encryption key [**Figure 1: 102A; Figure 4: 400; Specification: paragraph 0022, page 8, lines 3-19; paragraph 0023; page 8, line 20 to page 9, line 4; paragraph 0025, page 9, lines 18-27**].

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The following issues are presented to the Board of Appeals for decision:

(A) Whether Claims 1-41 are patentable under 35 U.S.C. 102(b) over U.S. Patent 5,706,348 (Gray).

VII. ARGUMENTS

A. Claims 1-41 are patentable under 35 U.S.C. 102(b) over U.S. Patent 5,706,348 (Gray)

1. Gray: Overview

Gray teaches a key synchronization technique in which marker cells (i.e. special purpose cells) notify a destination node that it is to activate a previously-received decryption key. Col. 4, lines 60-63. FIG. 5 illustrates the steps performed at the source node in maintaining key synchronization using one of two types of marker cells. Col. 4, lines 63-66. As indicated by Gray in col. 5, lines 7-13 (emphasis added),

> If a key update is to occur, the new decryption key is sent to the destination node in an operation 66 **using a conventional secure and reliable key exchange protocol**. The specific key exchange protocol employed is not critical to the present invention. It only matters that the new key is sent to the destination node at which it is eventually to be used.

2. Limitations recited in Claims 1-41 are not taught by Gray.

Appellant respectfully submits that Gray fails to disclose or suggest at least the following, explicitly-identified claim limitations. Specifically, Claim 1 recites, in part (emphasis added),

> sending from a first transceiver to a second transceiver a request to initiate derivation of a new encryption key, the request to **initiate a new encryption key derivation being controlled by a MAC sub-layer** and including an exchange threshold indicative of when the new encryption key is to be used to encrypt communication packets.

As taught by Appellant in paragraph [0006] of the Specification, a presentation layer or a session layer is typically used to initiate encrypted communication. The

presentation and the session layers are higher OSI (Open System Interconnection) layers than the MAC sub-layer, which forms part of the data link layer. See, e.g. presentation layer 106, session layer 105, and data link layer 102 of Figure 1. As further taught by Appellant in paragraph [0007] of the Specification:

> because MAC sub-layer 102A currently does not provide a mechanism to communicate to the higher layer that the key needs to be updated, the higher layer must redundantly store this information, monitor the state of the key (i.e. its location in the key space), and update the key independent of any communication with MAC sub-layer 102A. Moreover, because there is no defined protocol to update the key, the higher layer merely supplants the old key with a new key, thereby causing traffic disruption. Finally, the higher layer does not control communications regarding the data packet granularity (which is provided by MAC sub-layer 102A). Thus, the higher layer is unable to predict when repetition of nonces occurs (also known as collisions), which can undermine security.

Advantageously, in the recited method for encrypted communications, the request to **initiate a new encryption key derivation is controlled by a MAC sub-layer**. Thus, by using the recited method, the higher layer need not store the information regarding a key that needs updating, monitor the state of the key, or update the key independent of any communication with the MAC sub-layer.

Appellant respectfully submits that Gray fails to teach a MAC sub-layer that initiates derivation of a new key encryption. Indeed, **Gray fails to mention anything regarding a MAC layer, much less its advantages in initiating key encryption**. Because Gray fails to disclose or suggest a request to initiate a new encryption key derivation **being controlled by a MAC sub-layer**, Appellant requests reconsideration and withdrawal of the rejection of Claim 1.

Claims 2-25 depend from Claim 1 and therefore are patentable for at least the reasons presented for Claim 1. Based on those reasons, Appellant requests reconsideration and withdrawal of the rejection of Claims 2-9, 14, 16-17, and 20-25 as well as the objection to Claims 10-13, 15, and 18-19.

Claim 26 recites (emphasis added),

> a physical control layer that sends to the second transceiver a request to initiate derivation of a new encryption key, the request to **initiate a new encryption key derivation being controlled by a MAC sub-layer** and including an exchange threshold indicative of when the new encryption key is to be used to encrypt communication packets.

Therefore, Claim 26 is patentable for the same reasons presented for Claim 1. Based on those reasons, Appellant requests reconsideration and withdrawal of the rejection of Claim 26.

Claims 27-36 depend from Claim 26 and therefore are patentable for at least the reasons presented for Claim 26. Based on those reasons, Appellant requests reconsideration and withdrawal of the rejection of Claims 27-30, 33, and 35-36 as well as the objection to Claims 31-32 and 34.

Claim 37 recites in part (emphasis added),

> a physical control layer that receives from the second transceiver a request to initiate derivation of a new encryption key, the request to **initiate a new encryption key derivation being controlled by a MAC sub-layer** and including an exchange threshold indicative of when the new encryption key is to be used to encrypt communication packets, and **a first nonce needed to derive the new encryption key**.

Therefore, Claim 37 is also patentable for the same reasons presented for Claim 1. Moreover, Gray fails to disclose or suggest a nonce needed to derive the new encryption key. Based

on the above reasons, Appellant requests reconsideration and withdrawal of the rejection of Claim 37.

Claims 38-41 depend from Claim 37 and therefore are patentable for at least the reasons presented for Claim 37. Based on those reasons, Appellant requests reconsideration and withdrawal of the rejection of Claims 38 and 41 as well as the objection to Claims 39-40.

B. CONCLUSION

For the foregoing reasons, it is submitted that the Examiner's rejections of/objections to Claims 1-41 are erroneous, and reversal of these rejections is respectfully requested.

Respectfully submitted,

Customer No.: 30547

Jeanette S. Harms
Attorney for Appellant
Reg. No. 35,537

Telephone: 408-451-5907
Facsimile: 408-451-5908

VIII. CLAIMS APPENDIX

1. (Original) A method for encrypted communications between a first transceiver and a second transceiver, the method comprising.

sending from a first transceiver to a second transceiver a request to initiate derivation of a new encryption key, the request to initiate a new encryption key derivation being controlled by a MAC sub-layer and including an exchange threshold indicative of when the new encryption key is to be used to encrypt communication packets.

2. (Original) The method of claim 1, wherein the exchange threshold is a time.

3. (Original) The method of claim 1, wherein the exchange threshold is a counter value.

4. (Original) The method of claim 1, wherein the exchange threshold is a number of packets.

5. (Original) The method of claim 1, wherein the exchange threshold is at least one of a time, a counter value, and a number of packets.

6. (Original) The method of claim 1, wherein the request to initiate derivation of the new encryption key includes a timeout limit that indicates that a session is to be at least one of aborted or retried when the timeout limit is satisfied.

7. (Original) The method of claim 1, wherein the request to initiate derivation of the new encryption key is sent from the

first transceiver to the second transceiver and the new encryption key is to be generated at the second transceiver, in response to the request, before a key space of an old nonce value has been exhausted.

8. (Original) The method of claim 1, wherein the request to initiate derivation of the new encryption key includes a first nonce needed to derive the new encryption key.

9. (Previously Presented) The method of claim 8, further comprising:

sending from the second transceiver to the first transceiver, in response to the request to initiate derivation of the new encryption key, a second nonce needed to derive the new encryption key.

10. (Original) The method of claim 1, wherein the request to initiate derivation of the new encryption key includes a first transceiver authentication indication that authenticates the first transceiver to the second transceiver.

11. (Original) The method of claim 10, further comprising sending from the second transceiver to the first transceiver, in response to the request to initiate derivation of the new encryption key, a second transceiver authentication indication which authenticates the second transceiver to the first transceiver.

12. (Original) The method of claim 1, wherein the request to initiate derivation of the new encryption key includes a new initial nonce value that is used along with the new encryption key for encryption.

13. (Previously Presented) The method of claim 12, further comprising:

sending from the second transceiver, in response to the request to initiate derivation of the new encryption key, a status indicator indicative of the second transceiver's determination of the feasibility of being able to commence using the new encryption key at the second transceiver in accordance with the exchange threshold.

14. (Original) The method of claim 1, further comprising:

determining whether the new encryption key needs to be derived; and

wherein sending the request to initiate derivation of the new encryption key is based upon the determination of whether the new encryption key needs to be derived.

15. (Original) The method of claim 1, further comprising:

generating the new encryption key at the first transceiver and the second transceiver;

determining at at least one of the first transceiver and the second transceiver whether the exchange threshold has been satisfied; and

encrypting at at least one of the first transceiver and the second transceiver using the new encryption key when the exchange threshold has been satisfied.

16. (Original) The method of claim 15 further comprising:

continuing communication between the first transceiver and the second transceiver using for encryption an old encryption key generated before the new encryption key when the exchange threshold has still not been satisfied.

17. (Original) The method of claim 16 wherein encrypting using the new encryption key occurs without disrupting communication between the first transceiver and the second transceiver.

18. (Previously Presented) The method of Claim 1, wherein the request to initiate derivation of the new encryption key includes a first nonce needed to derive the new encryption key, the method further comprising:

sending from the second transceiver to the first transceiver, in response to the request to initiate derivation of the new encryption key, a second nonce needed to derive the new encryption key.

19. (Original) The method of claim 18, further comprising:

generating at at least one of the first transceiver and the second transceiver the new encryption key;

determining at at least one of the first transceiver and the second transceiver whether the exchange threshold has been satisfied; and

encrypting at at least one of the first transceiver and the second transceiver using the new encryption key when the exchange threshold has been satisfied.

20. (Original) The method of claim 19, wherein the request to initiate derivation of the new encryption key includes a new initial nonce value and encrypting includes using the initial nonce value and the new encryption key for encryption, the method further comprising:

determining whether the new encryption key needs to be derived; and

wherein sending the request to initiate derivation of the new encryption key is based upon the determination of whether the new encryption key needs to be derived.

21. (Previously Presented) The method of claim 20, the method comprising:

sending from the first receiver to the second transceiver a first transceiver authentication indication that authenticates the first transceiver to the second transceiver; and

sending from the second transceiver to the first transceiver a second transceiver authentication indication that authenticates the second transceiver to the first transceiver.

22. (Original) The method of claim 21, further comprising sending from the first transceiver to the second transceiver the second nonce.

23. (Original) The method of claim 22 further comprising:

continuing communication between the first transceiver and the second transceiver using an old encryption key generated before the new encryption key when the exchange threshold has still not been satisfied.

24. (Original) The method of claim 23 wherein encrypting using the new encryption key occurs without disrupting communication between the first transceiver and the second transceiver.

25. (Original) The method of claim 24, wherein the request to initiate derivation of the new encryption key includes a timeout limit that indicates that a communication is one of aborted and retried when the timeout limit is satisfied.

26. (Original) A first transceiver that is to conduct encrypted communications with a second transceiver, the first transceiver comprising:

a physical control layer that sends to the second transceiver a request to initiate derivation of a new encryption key, the request to initiate a new encryption key derivation being controlled by a MAC sub-layer and including an exchange threshold indicative of when the new encryption key is to be used to encrypt communication packets.

27. (Previously Presented) The first transceiver of claim 26, wherein the exchange threshold is a number of packets.

28. (Previously Presented) The first transceiver of claim 26, wherein the request includes a first transceiver identifier that authenticates the first transceiver to the second transceiver.

29. (Previously Presented) The first transceiver of claim 26, wherein the request to initiate derivation of the new encryption key includes a timeout limit that indicates that a session is to be at least one of aborted or retried when the timeout limit is satisfied.

30. (Previously Presented) The first transceiver of claim 26, wherein the request to initiate derivation of the new encryption key includes a first nonce needed to derive the new encryption key.

31. (Previously Presented) The first transceiver of claim 26, wherein the request to initiate derivation of the new

encryption key includes a first transceiver authentication indication that authenticates the first transceiver to the second transceiver.

32. (Previously Presented) The first transceiver of claim 26, wherein the request to initiate derivation of the new encryption key includes a new initial nonce value that is used in combination with the new encryption key for encryption.

33. (Previously Presented) The first transceiver of claim 26, wherein the physical control layer determines whether the new encryption key needs to be derived before sending the request to initiate derivation of the new encryption key; and

wherein sending the request to initiate derivation of the new encryption key is based upon the determination of whether the new encryption key needs to be derived.

34. (Previously Presented) The first transceiver of claim 26, wherein the physical layer receives a second nonce from the second transceiver, generates the new encryption key, determines whether the exchange threshold has been satisfied, and encrypts using the new encryption key when the exchange threshold has been satisfied.

35. (Original) The first transceiver of claim 34 wherein the physical control layer continues using for encryption an old encryption key generated before the new encryption key when the exchange threshold has still not been satisfied.

36. (Previously Presented) The first transceiver of claim 26, wherein the physical control layer sends the request early enough so that the new encryption key is to be generated at the

second transceiver, in response to the request, before a key space of an old nonce value has been exhausted.

37. (Original) A first transceiver that is to conduct encrypted communications with a second transceiver, the first transceiver comprising:

a physical control layer that receives from the second transceiver a request to initiate derivation of a new encryption key, the request to initiate a new encryption key derivation being controlled by a MAC sub-layer and including an exchange threshold indicative of when the new encryption key is to be used to encrypt communication packets, and a first nonce needed to derive the new encryption key.

38. (Original) The first transceiver of claim 37, wherein the physical control layer sends to the second transceiver, in response to the request to initiate derivation of the new encryption key, a second nonce.

39. (Original) The first transceiver of claim 37, wherein the physical control layer sends to the second transceiver, in response to the request to initiate derivation of the new encryption key, a status indication indicative of the first transceiver's determination of the feasibility of being able to commence using the new encryption key at the first transceiver in accordance with the exchange threshold.

40. (Previously Presented) The first transceiver of claim 37, wherein the physical control layer generates the new encryption key, determines whether the exchange threshold has been satisfied, and encrypts using the new encryption key when the exchange threshold has been satisfied.

41. (Previously Presented) The first transceiver of claim 39, wherein the physical control layer continues communication between the first transceiver and the second transceiver using for encryption an old encryption key generated before the new encryption key when the exchange threshold has still not been satisfied.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.